

REMARKS

By this Amendment, claims 1, 6 and 15-19 are amended, and claims 7-11 are cancelled. Claims 2-5 and 12-14 remain in the application. Thus, claims 1-6 and 12-19 are active in the application. Reexamination and reconsideration of the application are respectfully requested.

Minor editorial revisions have been made to the specification to correct misspelled words. The Applicants respectfully submit that no new matter has been added.

The Applicants thank the Examiner for conducting the interview with the Applicants' undersigned representative. Although no agreement could be reached on the allowability of the claims as presented in the September 1, 2005 Amendment, the Applicants appreciate the Examiner's comments on the application and the applied references. The Applicants will demonstrate in detail below why the present invention is patentable over the applied references.

In item 4 on page 4 of the Office Action, claims 1 and 3-19 were rejected under 35 U.S.C. § 102(e) as being anticipated by Dai (U.S. 6,081,598). This rejection is respectfully traversed for the following reasons.

The present invention provides a cryptocommunication system, method and program for ensuring the security of data transmission from third party attacks. The cryptocommunication system of the present invention includes a transmission apparatus and a reception apparatus. The cryptocommunication method and program of the present invention include a transmission operation and a reception operation.

Independent claim 1 recites the cryptocommunication system as including the transmission apparatus and the reception apparatus, independent claims 15-17 recite the transmission operation and reception operation of the present invention, and independent claim 18 recites the transmission apparatus of the present invention recited in claim 1.

As exemplarily shown in Figure 1, the transmission apparatus of the cryptocommunication system of the present invention includes first generating means for generating first additional information Ra. The transmission apparatus also includes first operation means for performing an invertible bit-connecting operation on plaintext m and the first additional information Ra so as to generate connected information F(m, Ra). The transmission apparatus of claim 1 also includes encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext E(F(m, Ra),

K_p, r), where K_p represents an encryption key used in the encryption algorithm, and r represents a random number that is generated and used in the encryption algorithm.

Accordingly, the first operation means performs the invertible bit-connecting operation on the plaintext m and the first additional information R_a to generate the connected information $F(m, R_a)$. Thus, the connected information generated by the first operation means can be represented as:

$F(m, R_a) = m \parallel R_a$, where the operator \parallel represents a bit-connecting operation.

Furthermore, the encrypting means encrypts the connected information $F(m, R_a)$ according to an encryption algorithm to generate the ciphertext $E(F(m, R_a), K_p, r)$.

Accordingly, the generated ciphertext $E(F(m, R_a), K_p, r)$ is the encrypted product of the connected information $F(m, R_a)$, which is the invertible bit-connected product of the plaintext m and the first additional information R_a . Therefore, in effect, the encrypting means encrypts the invertible bit-connected product of the plaintext m and the first additional information R_a . Thus, the ciphertext generated by the encrypting means can be represented as:

Ciphertext = $E(F(m, R_a), K_p, r)$

The Claimed Invention

Claims 1 and 18 each recite the transmission apparatus as comprising (1) first operation means for performing an invertible bit-connecting operation on the plaintext and the first additional information so as to generate connected information, and (2) encrypting means for encrypting the connected information according to an encryption algorithm so as to generate ciphertext.

Claims 15-17 each recite a transmission operation as comprising (1) performing an invertible bit-connecting operation on the plaintext and the first additional information to generate connected information, and (2) encrypting the connected information according to an encryption algorithm to generate ciphertext.

Accordingly, claims 1 and 15-18 each recite two distinct operations for generating the ciphertext. First, an invertible bit-connecting operation is performed on the plaintext and the first additional information to generate the connected information. Second, the connected information is encrypted to generate the ciphertext.

Therefore, in effect, claims 1 and 15-18 each recite that the invertible bit-connected product of the plaintext and the first additional information is encrypted.

As demonstrated above, the inventions of claims 1 and 15-18 each recite similar features of the present invention. In particular, the transmission operation recited in claims 15-17 corresponds to the operations that the elements of the transmission apparatus of claims 1 and 18 are defined to perform. Therefore, the following discussion primarily focuses on particular elements of the transmission apparatus of claim 1, but the Examiner is respectfully requested to observe that the following discussion of claim 1 also applies to the inventions of claims 15-18.

Outline of Argument

The transmission apparatus of the cryptocommunication system of claim 1 includes constituent elements X and Y.

1. A first assumption is made that Dai discloses a technology corresponding to element X. Under this first assumption, the Applicants will demonstrate that Dai does not disclose or suggest a technology corresponding to element Y.

2. A second assumption is made that Dai discloses a technology corresponding to element Y. Under this second assumption, the Applicants will demonstrate that Dai does not disclose or suggest a technology corresponding to element X.

According to this method of demonstrating that Dai fails to disclose or suggest each and every limitation of the transmission apparatus of claim 1, the Applicants will establish that Dai can only reasonably be interpreted as disclosing either element X or Y, and that the transmission apparatus of claim 1 is clearly distinguishable and novel over the technology disclosed in Dai.

Disclosure of Dai

Dai discloses a cryptographic system which includes an encoder 22 (transmission apparatus) and a decoder 24 (reception apparatus). The encoder 22 transforms a message M into ciphertext C and transmits the ciphertext C over a communications channel 26 to the decoder 24 (see Figure 1 and Column 2, lines 31-55). The encoder 22 of Dai also transmits a computed hash value $h_2(x, M)$ in addition to the ciphertext C to the decoder 24 (see steps 104-105 in Figure 3). However, it must be noted that the hash value $h_2(x, M)$ is not related to the creation of the

ciphertext C, and is merely disclosed as being transmitted to the decoder 24 in addition to the ciphertext C.

The ciphertext C of Dai is composed of two components, a value V and a value W. Dai discloses that the encoder 22 “packages the values V and W together to form the ciphertext C, and sends [the ciphertext C] across the communications channel 26 to the decoder 24” (see Column 4, lines 1-3).

Dai discloses that the value V is a function of a number x, or $V=x^e$, where e is an integer (see Column 2, lines 33-36, Column 3, lines 53-56 and step 102 of Figure 3).

Dai discloses that the “value W is encoded [(encrypted)] as a function of a value $h_1(x)$ and the message M (e.g., $h_1(x) \text{ xor } M$),” where “xor” is an exclusive OR function, and “ h_1 ” is a one-way function of the number x (see Column 2, lines 48-50, Column 3, lines 58-67, and step 102 of Figure 3).

Accordingly, since Dai discloses that the encoder “packages the values V and W together to form the ciphertext C,” (see Column 4, lines 1-2), the ciphertext C of Dai can be represented as:

$$C = V + W, \text{ or}$$

$$C = (x^e) + (h_1(x) \text{ xor } M)$$

Comparison and Analysis of Claim 1 and Dai Under First and Second Assumptions

(1) Comparison and Analysis Under First Assumption

As mentioned above, Dai discloses that the message M is encrypted by using a value W, where $W = (h_1(x) \text{ xor } M)$.

“xor” is considered to correspond to an encryption algorithm. In view of this, under the first assumption, the value $W = (h_1(x) \text{ xor } M)$ is considered to correspond to the encrypting means of claim 1.

Under this first assumption, the encoder 22 disclosed in Dai transmits the ciphertext C that includes the value W and the value V ($C = V + W$). However, while the value W would correspond to the encryption means under this first assumption, Dai does not disclose or suggest anything remotely resembling the operation of generating the connected information as recited in claim 1.

In particular, assuming that the value $W = (h_1(x) \text{ xor } M)$ is considered to correspond to the encrypting means of claim 1, Dai does not disclose, suggest or even contemplate that any operation is performed on the message M to result in the “connected information” recited in claim 1.

On the other hand, claim 1 recites two distinct operations for generating the ciphertext. First, an invertible bit-connecting operation is performed on the plaintext and the first additional information to generate the connected information. Second, the connected information is encrypted to generate the ciphertext. Accordingly, claim 1 clearly recites that the invertible bit-connected product of the plaintext and the first additional information is encrypted in order to generate the ciphertext.

However, in contrast to claim 1, Dai does not perform any operation whatsoever on the message M if it assumed that the value $W = (h_1(x) \text{ xor } M)$ corresponds to the encrypting means of claim 1.

Therefore, under this first assumption, Dai clearly does not disclose or suggest a technology of generating the connected information from the message M because Dai does not perform any other operations on the message M. That is, under the first assumption, Dai cannot be reasonably interpreted as disclosing “first operation means for performing an invertible bit-connecting operation on the plaintext and the first additional information to generate connected information,” as recited in claim 1.

The cryptocommunication system of claim 1 produces a novel and advantageous effect of generating ciphertext whose security level is high, by providing the first operation means for performing an invertible bit-connecting operation on the plaintext and the first additional information to generate connected information, and the encrypting means for encrypting the connecting information to generate encrypted connected information.

Under this first assumption, it is assumed that the value $W = h_1(x) \text{ xor } M$ corresponds to the encrypting means of claim 1. Under this first assumption, Dai cannot reasonably be interpreted as disclosing the first operation means of claim 1 for the following reasons.

Using this first assumption, suppose that a third party intercepts the ciphertext C that is generated according to the system of Dai. Under this first assumption, Dai does not disclose or suggest a technology of generating the connected information from the message M because Dai does not perform any other operations on the message M. As a result, Dai cannot prevent the

third party from obtaining the message by decrypting the ciphertext C, since Dai does not disclose or suggest a technology of the generating connected information from the message M because Dai does not perform any other operations on the message M. Accordingly, Dai cannot reasonably be interpreted as disclosing or suggesting “first operation means for performing an invertible bit-connecting operation on the plaintext and the first additional information to generate connected information,” as recited in claim 1.

(2) Comparison and Analysis Under Second Assumption

In line 6 on page 5 of the Office Action, the Examiner alleged that “x” corresponds to the first additional information of claim 1. If this is assumed to be the case, the value $W = h_1(x) \text{ xor } M$ corresponds to the invertible operation of the first operation means of claim 1, and the value W corresponds to the connected information.

However, under this second assumption, the encoder 22 of Dai does not perform any operation whatsoever with respect to the value W, and therefore, the value W is transmitted without being encrypted. Therefore, if $W = h_1(x) \text{ xor } M$ is considered to correspond to the invertible operation of claim 1 and the value W is considered to correspond to the connected information of claim 1, Dai cannot be reasonably interpreted as disclosing an “encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext,” as recited in claim 1, since Dai performs no operation whatsoever with respect to the connected information W.

Accordingly, under this second assumption, the value W will be transmitted without being encrypted, and as a result, the system of Dai cannot maintain the secrecy of the transmitted information.

In contrast to Dai, the transmission apparatus of claim 1 includes both the first operation means and the encrypting means. As a result, information that is to be transmitted is made secret because of being encrypted by the encrypting means before the information is transmitted. In addition, the encrypting means of claim 1 encrypts connected information, and therefore is able to prevent the third party that has intercepted the ciphertext from obtaining the corresponding message, even if the intercepted ciphertext has been successfully decrypted.

Thus, the invention of claim 1 has an effect of generating ciphertext whose security level is high, and therefore, the invention of claim 1 has marked technological advantages over the system disclosed in Dai.

Moreover, regardless of whether the first assumption or the second assumption is used, Dai clearly does not disclose or suggest performing an invertible bit-connecting operation on the message M and the first additional information. In particular, regardless of whether $W = h_1(x)$ xor M is considered to correspond to the first operation means or the encrypting means of claim 1, Dai does not even contemplate performing a invertible bit-connecting operation on any two values of data.

(3) Summary of the Comparison and Analysis Under the First and Second Assumptions

As described above, if “the value $W = h_1(x)$ xor M” is assumed to correspond to the encrypting means of claim 1, Dai clearly fails to disclose or suggest the first operation means of claim 1 since Dai does not disclose or suggest generating the connected information from the message M, as Dai does not perform any other operations on the message M. Therefore, under the first assumption, Dai cannot be reasonably interpreted as disclosing first operation means for performing an invertible bit-connecting operation on the plaintext and the first additional information to generate connected information, as recited in claim 1.

On the other hand, if, under the second assumption, “the value $W = h_1(x)$ xor M” is assumed to correspond to the first operation means of claim 1, Dai fails to disclose or suggest the encrypting means of claim 1, since Dai performs no operation whatsoever with respect to the connected information W. Accordingly, if “the value $W = h_1(x)$ xor M” is assumed to correspond to the first operation means of claim 1, Dai cannot be reasonably interpreted as disclosing encrypting means for encrypting the connected information according to an encryption algorithm so as to generate the ciphertext, as recited in claim 1.

In view of the above, Dai clearly does not disclose or suggest a combination of the first operation means and the encrypting means of claim 1. Similarly, Dai does not disclose or suggest a combination of the first operation means and the encrypting means of the transmission apparatus of claim 18.

Furthermore, for the foregoing reasons, Dai clearly does not disclose or suggest a combination of operations of performing an invertible bit-connecting operation on the plaintext

and the first additional information to generate connected information, and encrypting the connected information according to an encryption algorithm to generate the ciphertext, as recited in the method and programs of claims 15-17.

Accordingly, the inventions of claims 1 and 15-18 are clearly not anticipated by Dai since Dai does not disclose each and every limitation of claims 1 and 15-18.

Furthermore, because of the clear distinctions discussed above, one skilled in the art would not have been motivated to modify the system of Dai to provide for either the first operation means or method and program element of claims 1 and 15-18 or the encrypting means or method and program element of claims 1 and 15-18 to arrive at the inventions of claims 1 and 15-18.

Accordingly, claims 1 and 15-18 are clearly not anticipated or rendered obvious by Dai since Dai fails to disclose or suggest each and every limitation of claims 1 and 15-18.

In item 8 on page 6 of the Office Action, claim 2 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Wei Dai in view of Jones (5,412,730). As demonstrated above, Dai clearly fails to disclose or suggest the first operation means and the encrypting means of claims 1 and 18, as well as the corresponding operations of the program and method of claims 15-17.

Jones also fails to disclose or suggest the first operation means and encrypting means of claims 1 and 18 as well as the corresponding operations of the program and method of claims 15-17.

Therefore, Jones does not cure the deficiencies of Dai for failing to disclose or suggest each and every limitation of claims 1 and 15-18.

Accordingly, no obvious combination of Dai and Jones would result in the inventions of claims 1 and 15-18 since Dai and Jones, either individually or in combination, clearly fail to disclose or suggest each and every limitation of claims 1 and 15-18.

Furthermore, it is submitted that the clear distinctions discussed above are such that a person having ordinary skill in the art at the time the invention was made would not have been motivated to modify Dai and Jones in such a manner as to result in, or otherwise render obvious, the present invention as recited in claims 1 and 15-18. Therefore, it is submitted that the claims 1 and 15-18, as well as claims 2-6, 12-14 and 19 which depend therefrom, are clearly allowable over the prior art as applied by the Examiner.

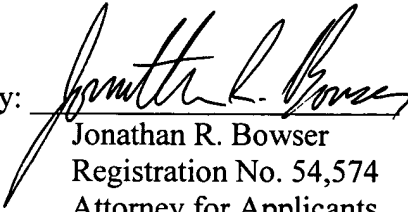
In view of the foregoing amendments and remarks, it is respectfully submitted that the present application is clearly in condition for allowance. An early notice thereof is respectfully solicited.

If, after reviewing this Amendment, the Examiner feels there are any issues remaining which must be resolved before the application can be passed to issue, the Examiner is respectfully requested to contact the undersigned by telephone in order to resolve such issues.

Respectfully submitted,

Masato YAMAMICHI et al.

By:


Jonathan R. Bowser
Registration No. 54,574
Attorney for Applicants

JRB/nrj
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
May 15, 2006